# SOCIÁLNE INŽINIERSTVO

Ľudské správanie je jednou z najslabších článkov v počítačovej bezpečnosti organizácie a preto je nutné ho pravidelne testovať. Sociálne inžinierstvo umožňuje psychologickú manipuláciu ľudí na vykonanie nechcených akcií.

Služba zahŕňa viacero druhov phishingových útokov a to pomocou telefonátov, zaslaných smsiek a e-mailových správ, ktorých cieľom je prinútiť zamestnanca prezradiť citlivé informácie alebo vykonať škodlivé/neúmyselné akcie (napríklad vyzradenie svojho hesla, spustenie škodlivého kódu, otvorenie "vstupnej brány" do spoločnosti.. ). Na testy používame náš interne vyvinutý framework a metodológiu, ktorá simuluje útok tak, ako by postupoval skutočný útočník.

## PREHĽAD SLUŽBY

Cieľom testov pomocou sociálneho inžinierstva je overiť povedomie zamestnancov o bezpečnosti. Výsledkom testu je report, ktorý obsahuje detailnú analýzu vykonaných testov s manažérskym zhrnutím.

Cena testu pomocou sociálneho inžinierstva záleží od hĺbky a komplexnosti testov, veľkosti testovanej spoločnosti. Táto cena je určená po konzultácii so zákazníkom, v ktorom sa určí rozsah, typ testov a ďalšie požiadavky od zákazníka.

Test môže byt vykonaný pomocou metódy BLACK BOX (žiadne informácie o testovanej spoločnosti), GREY BOX (čiastočné informácie o testovanej spoločnosti) alebo WHITE BOX (všetky potrebné informácie o testovanej spoločnosti). V závislosti od dohodnutej metódy bude prispôsobená prvá fáza testu, ktorá sa zaoberá zberom informácii o testovacej spoločnosti (informácie o zamestnancoch z verejne dostupných zdrojov/sociálnych sieti, používaných IT prostriedkoch..).

Ponúkame viacero druhov testov, ktoré sa líšia rozsahom a hĺbkou vykonaného testu. Po diskusii so zákazníkom odporučíme typ a rozsah vhodného testu pre konkrétnu spoločnosť.

## PHISHING TEST

- Phishingový test - phishingová kampaň na všetkých zamestnancov spoločnosti
- Spear phishing test - cielený phishingový test na úzku skupinu ľudí v spoločnosti

Phishingový/spear phishigový email sa pokúša donútiť testované osoby spraviť nechcenú akciu (zmena hesla, navštívenie webovej stránky so škodlivým kódom (drive-by útok), navštívenie falošnej stránky, stiahnutie prílohy a následné spustenie škodlivého kódu (RAT, ransomware, keylogger,.. ).

## VISHING/SMS PHISHING

Na rozdiel od klasického phishingu, je tento typ phishingu vykonaný pomocou telefonátu alebo zaslanej SMSky. Cieľom tohto typu útoku je taktiež pokus o získanie dôverných, obchodných dát, alebo vykonať nechcenú akciu (zmena hesla, ...). V prípade, že je to možné, caller/sender ID je sfalšované (spoofované).

## FYZICKÝ/ON-SITE (BAITING)

Fyzická obdoba testu sociálneho inžinierstva, v rámci ktorej sa v okolí objektu (budovy) testovanej spoločnosti porozhadzujú prenosné média (CD, DVD, USB kľúče). Na týchto médiách sa nachádza škodlivý kód (RAT, ransomware, keylogger,..) alebo len spustiteľný kód, ktorý poslúži na záverečné vyhodnotenie testu.